

ASV Scan Report Attestation of Scan Compliance

A1. Scan Customer Information				A2. Approved Scanning Vendor Information			
Company:	Open Tech Alliance, Storage Treasurers			Company:	TechSlayers LLC		
Contact Name:	Davin Dameron	Job Title:	CIO	Contact Name:	Walter Magana	Job Title:	VP Managed Services
Telephone:	N/A	Email:	ddameron@opentechalliance.com	Direct email:	wally@Techslayers.com	Support Email:	support@Techslayers.com
Business Address:	2101 West Peoria Ave, Suite 100			Business Address:	2201 E Camelback Rd		
City:	Phoenix	State/Province:	Arizona	City:	Phoenix	State/Province:	Arizona
ZIP/postal code:	85029	Country:	United States of America	ZIP/postal code:	85016	Country:	United States of America
URL:	opentechalliance.com			URL:	techslayers.com		

A3. Scan Status			
Date scan completed	09/01/2024	Scan expiration date (90 days from date scan completed)	12/01/2024
Compliance Status	PASS	Scan report type	Full scan
Number of unique in-scope components scanned			4
Number of identified failing vulnerabilities			0
Number of components found by ASV but not scanned because scan customer confirmed components were out of scope			0

A.4 Scan Customer Attestation

Open Tech Alliance attests on 09/01/2024 that this scan (either by itself or combined with multiple, partial, or failed scans/rescans, as indicated in the above Section A.3, "Scan Status") includes all components which should be in scope for PCI DSS, any component considered out of scope for this scan is properly segmented from my cardholder data environment, and any evidence submitted to the ASV to resolve scan exceptions -including compensating controls if applicable- is accurate and complete.

Open Tech Alliance also acknowledges 1) accurate and complete scoping of this external scan is my responsibility, and 2) this scan result only indicates whether or not my scanned systems are compliant with the external vulnerability scan requirement of PCI DSS; this scan result does not represent my overall compliance status with PCI DSS or provide any indication of compliance with other PCI DSS requirements.

A.5 ASV Attestation

This scan and report was prepared and conducted by TechSlayers LLC in collaboration with contractors and subcontractors including tenable according to internal processes that meet PCI DSS requirement 11.2.2 and the ASV Program Guide.

TechSlayers attests that the PCI DSS scan process was followed, including a manual or automated Quality Assurance process with customer boarding and scoping practices, review of results for anomalies, and review and correction of 1) disputed or incomplete results, 2) false positives, 3) compensating controls (if applicable), and 4) active scan interference. This report and any exceptions were reviewed by a TechSlayers developer and two other qualified third party assessors for PCI compliance. For further details please email brandon@techslayers.com

Manual Review and Inspection Attestation

Tech Slayers reviewed results of OpenTech Alliance most recent quarterly scans, penetration tests, and Facilities, all findings and reviews completed by a certified ASV vendor Tenable to confirm they covered all externally accessible (Internet-facing) IP addresses within the scope of the PCI DSS review and that the results of these scans were passing. Reviews of these security scans indicate that OpenTech Alliance is compliant with the PCI ASV Scan validation requirements. Additionally, their organizations commitment to improving security exceeds PCI Market expectations and their security readiness has improved over time.

ASV Scan Report Summary

Part 1. Scan Information

Scan Customer Company:	Open Tech Alliance	ASV Company:	Tenable
Date scan was completed:	09/01/2024	Scan expiration date:	12/01/2024

Part 2. Component Compliance Summary

Opentechalliance.com	PASS
Storage-treasures.com	PASS
72.44.248.98	PASS
72.44.248.101	PASS

Part 3. PCI DSS v3.2.1 Compliance Controls Validated

Install and maintain a firewall configuration to protect data	PASS
Do not use vendor-supplied defaults	PASS
Protect stored data	PASS
Encrypt transmission of CHD across public networks	PASS
Use and regularly update antivirus software	PASS
Develop and maintain secure systems and applications	PASS
Restrict access to data by business need-to-know	PASS
Assign a unique ID to each person with computer access	PASS
Restrict physical access to cardholder data	PASS
Track and monitor all access to network resources and CHD	PASS
Regularly test security systems and processes	PASS
Maintain a security policy that addresses information security for workers	PASS

All data and information provided and all analyses completed have been carefully reviewed by OpenTech Alliance, Tech Slayers, and at least one Tech Slayers Partner PCI Approved Scanning Vendor. All inputs and reports related to this PCI Assessment and Accreditation, to the best of our knowledge, accurately reflect OpenTech Alliance's current state of PCI compliance and on going commitment to customer data security.

TechSlayers LLC,

By: Walter Magana

Its: VP Managed Services

Date: 09/01/2024

Signature:

